

P2, L13 F05-517
I.D.S.

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-290149

(43)公開日 平成5年(1993)11月5日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/62	4 6 0	9071-5L		
12/14	3 2 0 B	9293-5B		
// G 0 6 F 12/00	5 3 7 H	7232-5B		

審査請求 未請求 請求項の数 2 (全 7 頁)

(21)出願番号 特願平4-91404

(22)出願日 平成4年(1992)4月13日

(71)出願人 000102728

エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目3番3号

(72)発明者 李 暎▲ソン▼

東京都港区虎ノ門1丁目26番5号 エヌ・
ティ・ティ・データ通信株式会社内

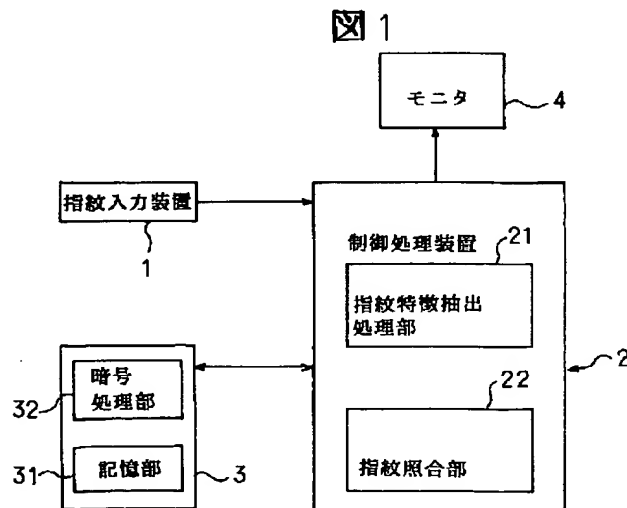
(74)代理人 弁理士 秋田 収喜

(54)【発明の名称】 指紋照合認証方式及びその装置

(57)【要約】

【目的】 指紋照合によって個人を認証するに際し、個人のプライバシーを保護し、悪用の危険性をなくする。

【構成】 登録する指紋情報は暗号化して登録し、かつ照合要求のあった個人の指紋情報は暗号化した後、登録された指紋情報と照合する。



【特許請求の範囲】

【請求項 1】 予め登録しておいた指紋情報と照合要求のあった個人の指紋情報とを照合し、個人の認証を行う指紋照合認証方式において、登録する指紋情報は暗号化して登録し、かつ照合要求のあった個人の指紋情報は暗号化した後、登録された指紋情報と照合することを特徴とする指紋照合認証方式。

【請求項 2】 予め登録しておいた指紋情報と照合要求のあった個人の指紋情報とを照合し、個人の認証を行う指紋照合認証装置において、個人の指紋を光学的に読み取る指紋入力手段と、読み取られた指紋の情報の特徴を抽出する特徴抽出手段と、この特徴抽出手段で抽出した指紋の特徴を暗号化する暗号化手段と、この暗号化手段で暗号化した指紋情報を記憶する記憶手段と、個人の認証を行うに際して前記指紋入力手段で読み取られ、かつ前記特徴抽出手段で特徴が抽出された後に前記暗号化手段で暗号化された個人の指紋情報と前記記憶手段に記憶された暗号化指紋情報とを照合し、その照合結果を出力する照合手段とを備えて成る指紋照合認証装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、予め登録しておいた指紋情報と照合要求のあった個人の指紋情報とを照合し、個人の認証を行う指紋照合認証方式およびその装置に関するものである。

【0002】

【従来の技術】 従来において、金融機関や原子力施設などの高いセキュリティを必要とする施設においては、予め登録されている個人のみの入室を許可するために、個人の指紋情報を用いた認証方法を採用している例がある。

【0003】 すなわち、個人の指紋パターンは隆線が枝分かれする位置や数、終端する位置が個人別に異なるという特徴を持っていることから、このような特徴点を抽出し、この特徴点のデータをそのまま指紋情報として登録しておき、入室を希望する個人による照合要求があったならば、その個人の指の指紋情報を読み取らせ、予め登録されている指紋情報と照合し、誤差が許容範囲内であれば、入室を許可された者と認定し、ドアロック等を解除して入室させるというものである。

【0004】

【発明が解決しようとする課題】 しかしながら、この従来の方法では、指紋情報が高度なプライバシーに属する情報であるにも関わらず、指紋情報をオリジナルのまま登録し、かつ照合しているため、登録者の心理的抵抗が大きい。例えば、照合時に指紋情報を通信回線やメモリ上に出力した時に外部からハッカーが侵入すれば、指紋情報が盗まれてしまい、プライバシーを侵害してしまうという危険性があった。その上、高度な技術を有する者が登録されている指紋情報から元の指紋パターンを復元

し、悪用する危険性もあった。

【0005】 本発明の目的は、個人のプライバシーを保護し、悪用される危険性のない指紋照合認証方式およびその装置を提供することである。

【0006】

【課題を解決するための手段】 上記目的を達成するために登録する指紋情報は暗号化して登録し、かつ照合要求のあった個人の指紋情報は暗号化した後、登録された指紋情報と照合することを特徴とする。

10 【0007】 また、本発明の指紋照合認証装置は、個人の指紋を光学的に読み取る指紋入力手段と、読み取られた指紋の情報の特徴を抽出する特徴抽出手段と、この特徴抽出手段で抽出した指紋の特徴を暗号化する暗号化手段と、この暗号化手段で暗号化した指紋情報を記憶する記憶手段と、個人の認証を行うに際して前記指紋入力手段で読み取られ、かつ前記特徴抽出手段で特徴が抽出された後に前記暗号化手段で暗号化された個人の指紋情報と前記記憶手段に記憶された暗号化指紋情報とを照合し、その照合結果を出力する照合手段とを具備させた。

20 【0008】

【作用】 上記手段によれば、指紋照合に用いる指紋情報は暗号化して登録し、かつ照合時にも暗号化したままの状態では照合するため、指紋のオリジナル情報が漏洩したり、盗まれて悪用される恐れがなくなり、個人のプライバシーを確実に保護することができる。

【0009】

【実施例】 以下、本発明の実施例を図面を用いて詳細に説明する。

30 【0010】 図 1 は本発明による指紋照合認証装置の一実施例を示すブロック図である。本実施例の指紋照合装置は、例えば光学的画像用読み取り装置等からなる指紋入力装置 1、コンピュータからなる制御処理装置 2、暗号処理部を有する IC カード等の記憶媒体 3、登録する指紋情報を表示するモニタ 4 で構成されている。

【0011】 このうち、制御処理装置 2 は指紋パターンから照合時に用いる特徴点を抽出するアルゴリズムで構成される指紋特徴抽出処理部 21 とマッチング処理を行う指紋照合部 22 とを有している。

40 【0012】 また、記憶媒体 3 は、記憶部 31 と暗号処理部 32 とで構成され、この暗号処理部 32 は所定の暗号関数によって指紋情報を暗号化するように構成されている。

50 【0013】 さらに、指紋入力装置 1 は図 2 に示すように、プリズム 11 の斜面に置かれた指 11 の指紋形成面に光源 12 から光を照射することにより、指紋形成面における隆線部分では「暗」、その他の部分では「明」となる図 3 に示すような指紋画像 13 を取り出し、この指紋画像 13 をテレビカメラ 14 で撮像し、AD 変換器 15 によってディジタルの指紋画像データに変換して制御処理装置 2 に入力するように構成されている。

3

【0014】このような構成の指紋入力装置1から指紋画像データを受けた制御処理装置2は、指紋特徴抽出処理部21において細線化処理を行って図4に示すような指紋画像データに変換し、特徴点の抽出を行う。

【0015】すなわち、指紋パターンは図4に記号40で示すように、隆線が枝分かれする位置やその数、および記号41で示すように終端する位置が個人別に異なるという特徴を持っていることから、このような特徴点を抽出し、この特徴点のデータをオリジナル指紋情報FPとして抽出する。

【0016】このオリジナル指紋情報FPは、ICカードで構成される記憶媒体3の暗号処理部32に送られ、ここで暗号関数Fで暗号化される。この場合の暗号文[FP]は数式(1)で示すことができる。

【0017】

$$[\text{数1}] \quad [FP] = F(FP) \quad (1)$$

但し、Fは暗号関数

そして、この暗号文[FP]は記憶部31に登録される。

【0018】この場合、細線化した指紋画像データは図5に示すように複数のブロックBn(図5の例ではB1~B9)に分割され、各ブロック別の特徴点が抽出され、その特徴点のデータを暗号関数Fで暗号化し、ブロック別の暗号文[FBn]に登録するようになっている。

$$[FP] = FB1 + FB2 + FB3 + \dots + FBn \quad (2)$$

となる。

【0026】次に、図7の照合処理動作においては、指紋入力装置1のプリズム10に置かれた照合要求のある指11の指紋画像をテレビカメラ14で撮像し、AD変換器15によってデジタルの指紋画像データに変換して制御処理装置2に入力し、指紋特徴抽出処理部21において細線化処理を行って図4に示すような指紋画像データに変換し、特徴点の抽出を行う。その後、抽出された特徴点のデータに基づきオリジナル指紋情報FP'を生成し、このオリジナル指紋情報FP'を記憶媒体3の

$$[FP'] = FB1' + FB2' + FB3' + \dots + FBn' \quad (3)$$

として表わすことができる。

【0030】次に、照合要求を行った個人が所有している記憶媒体3に登録されている暗号文を入力する。これは、図5で説明したように、暗号文[FP]がブロックBn別に生成されるため、ブロックBn別に入力する(ステップ71)。

【0031】次に、全ブロックの暗号文[FP]の入力が終了したかどうかを判定し、終了していなければ、ブロックポインタが現在示しているブロックの暗号文[FBn]を入力する(ステップ73)。

【0032】次に、記憶媒体3から読み込んだ暗号文[FP]と照合要求のあった暗号文[FP']とをそれぞれ対応するブロックの暗号文[FBn]、[FB

4

【0019】図6はこの実施例の指紋登録処理動作を示すフローチャートであり、図7は指紋照合処理動作を示すフローチャートである。

【0020】以下、各フローチャートを参照して指紋登録処理動作と指紋照合処理動作を説明する。

【0021】まず、図6の指紋登録処理動作においては、指紋入力装置1のプリズム10に置かれた指紋登録要求のある指11の指紋画像をテレビカメラ14で撮像し、AD変換器15によってデジタルの指紋画像データに変換して制御処理装置2に入力する(ステップ60, 61)。

【0022】次に、指紋特徴抽出処理部21において細線化処理を行って図4に示すような指紋画像データに変換し、特徴点の抽出を行う(ステップ62, 63)。

【0023】次に、抽出された特徴点のデータに基づきオリジナル指紋情報FPを生成する(ステップ64)。

【0024】次に、オリジナル指紋情報FPを図5に示したように複数のブロックBnに分割し、記憶媒体3の暗号処理部32に送り、暗号関数Fで暗号化させる(ステップ65)。この暗号化処理によって生成された暗号文[FBn]は記憶部31に登録される(ステップ66)。

【0025】

【数2】ここで、全体の暗号文[FP]は

暗号処理部32に送り、暗号関数Fで暗号化させる(ステップ70)。

【0027】すなわち、図6のステップ60からステップ65までと同様の処理を行い、照合要求のある指紋の暗号文を生成する。ここで、生成された照合要求のある暗号文を[FP']とする。

【0028】この暗号文[FP']もブロック別に生成されるので、

【0029】

【数3】

n']同士で比較し(ステップ74)、一致する場合は一致ブロック数Mを更新する(ステップ75)。すなわち、M=M+1とする。しかし、一致しない場合は何もしない。

【0033】次に、次のブロックの照合を行うべく、ブロックポインタを更新し、ステップ72に戻る(ステップ76)。

【0034】このような処理を繰返し行うことにより、全ブロックの暗号文[FBn]、[FBn']の照合が終了したならば、一致ブロック数Mとしいき値M'とを比較し、M>M'ならば、照合成功を表わす信号を出力する。しかし、M<M'ならば照合失敗を表わす信号を出力する(ステップ77)。

5

【0035】ここで、しきい値 M' は照合の成否を決定する基準値となるものであり、例えば n 個のブロックのうち80%以上の数のブロックが一致した時に照合成功となるように設定されている。

【0036】なお、しきい値 M' は個人の指紋の特徴を十分に網羅して得られた個人しきい値を用いることができる。

【0037】このように本実施例の指紋照合認証装置は、指紋照合に用いる指紋情報は暗号化して登録し、かつ照合時にも暗号化したままの状態では照合するため、指紋のオリジナル情報が漏洩したり、盗まれて悪用される恐れがなくなり、個人のプライバシーを確実に保護することができる。

【0038】なお、暗号化した指紋情報の暗号文は、ICカードから構成された記憶媒体3に登録しているが、メモ리카ード等の記録媒体に登録するようにすることができる。メモ리카ードを用いた場合は、暗号処理部32は指紋特徴抽出処理部21内に設ければよい。

【0039】また、暗号化関数は秘密鍵公開暗号アルゴリズムを用いれば、個人一人一人の指紋情報を秘密型個別鍵で暗号化を行うため、セキュリティがさらに高くなる。

【0040】

【発明の効果】以上説明したように本発明は、登録する指紋情報は暗号化して登録し、かつ照合要求のあった個

6

人の指紋情報は暗号化した後、登録された指紋情報と照合するように構成したため、指紋のオリジナル情報が漏洩したり、盗まれて悪用される恐れがなくなり、個人のプライバシーを確実に保護することができる。

【図面の簡単な説明】

【図1】 本発明による指紋照合認証装置の位置実施例を示すブロック図である。

【図2】 指紋入力装置の一例を示す構成図である。

【図3】 指紋入力装置で入力される指紋画像の一例を示す説明図である。

【図4】 指紋画像を細線化した画像を示す説明図である。

【図5】 指紋画像を暗号化するための領域分割例を示す説明図である。

【図6】 指紋情報の登録処理を示すフローチャートである。

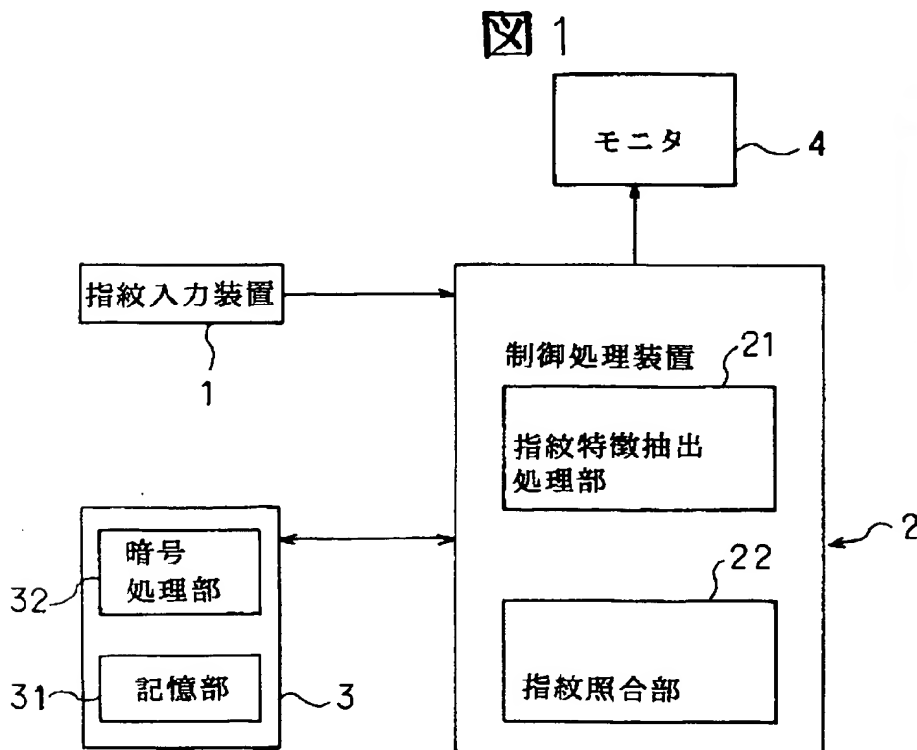
【図7】 指紋情報の照合処理を示すフローチャートである。

【符号の説明】

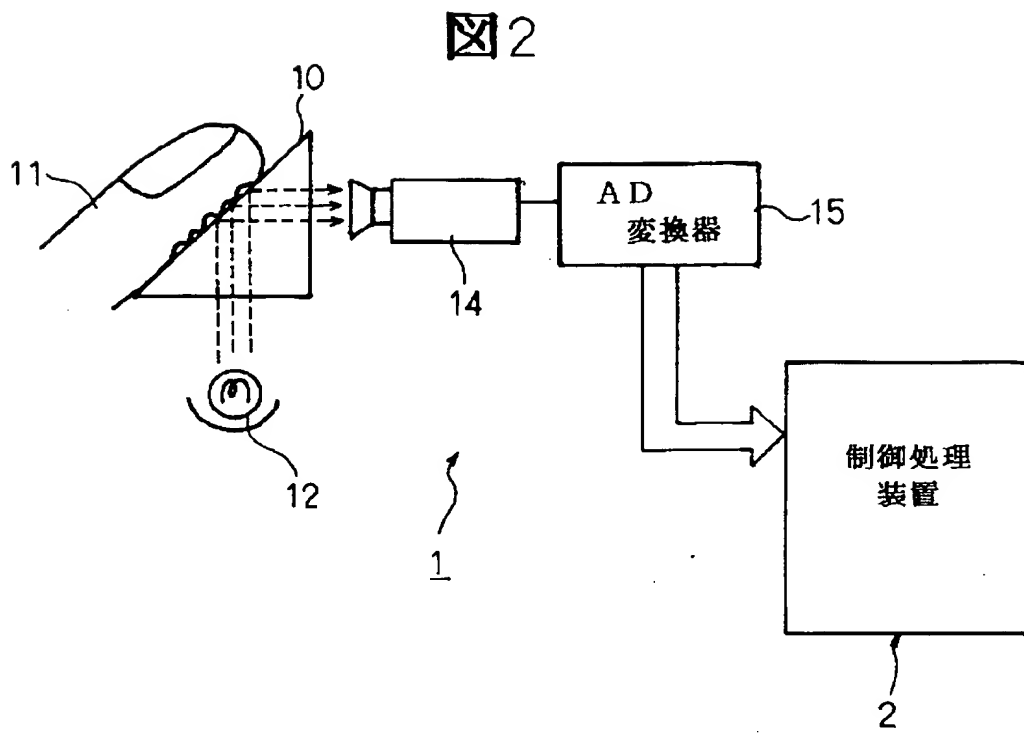
1…指紋入力装置、2…制御処理装置、3…記憶媒体、4…モニタ、10…プリズム、11…指、12…光源、13…指紋画像、14…テレビカメラ、15…AD変換器、21…指紋特徴抽出処理部、22…指紋照合部、31…記憶部、32…暗号処理部。

【図1】

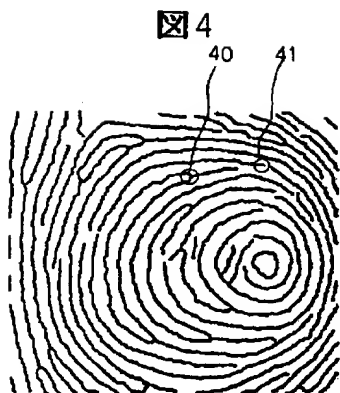
【図3】



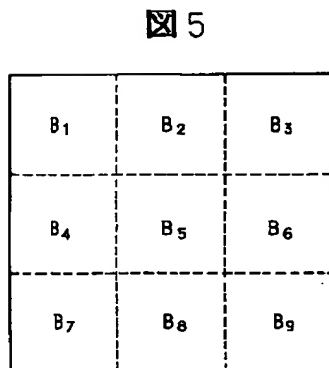
【図2】



【図4】

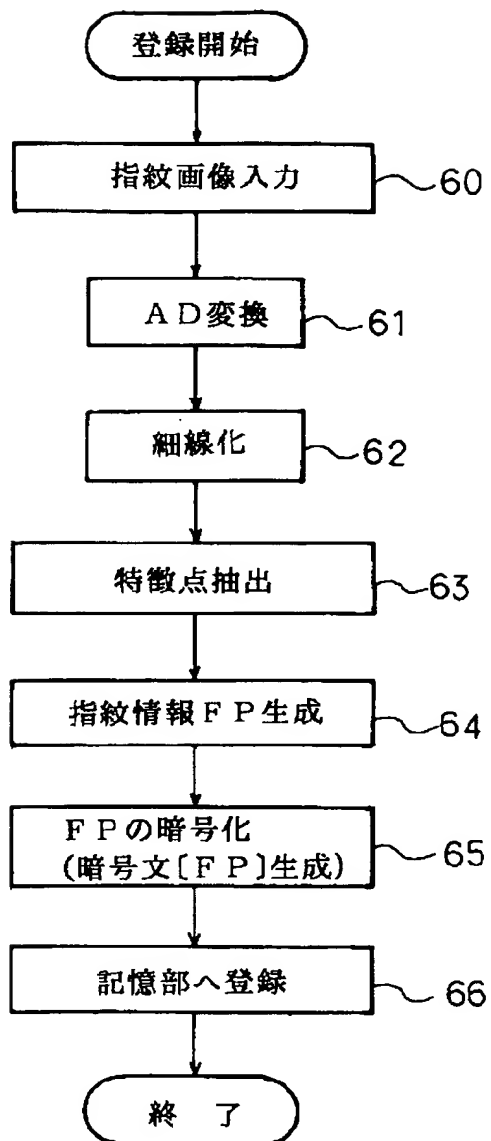


【図5】



【図6】

図 6



【図7】

図7

